STRATEGY RESEARCH PROJECT

SMART CARDS: AN ENABLER FOR ARMY PERSONNEL TRANSFORMATION

BY

MR. JAMES L. CALL, JR.
Department of the Army

USAWC CLASS OF 2001

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

SMART CARDS: AN ENABLER FOR ARMY PERSONNEL TRANSFORMATION

by

Mr. James L. Call, Jr.
U.S. Army

Colonel Ruth B. Collins
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

(This page is intentionally blank.)

ABSTRACT

AUTHOR: Mr. James L. Call, Jr.

TITLE: **SMART CARDS: AN ENABLER FOR ARMY PERSONNEL TRANSFORMATION**

FORMAT: Strategy Research Project

DATE: 10 April 2001 PAGES: 22 CLASSIFICATION: Unclassified

A critical element affecting Army readiness is personnel support. Personnel information on the battlefield and across all levels of the Army is necessary to support the force and to enable senior leaders to make wise decisions regarding the force. Personnel support involves accounting for people assigned to the Army, managing their careers, and providing service and well-being to families, retirees and veterans. A major part of the Army's current transformation involves redesign of personnel systems. Redesign involves moving into an easily accessible and comprehensive personnel system for all components of the Army and the Services. Emerging 21st Century technologies are aiding the Army's transformation to the objective force and the smart card is an integral part of this. Technological advancements such as the smart card will significantly enhance the Army's objective force to provide a more lethal, survivable, sustainable, deployable, and mobile force. Employing smart card technology is one aspect of keeping pace with the demand for accurate and timely military personnel information.

(This page intentionally blank.)

TABLE OF CONTENTS

ABSTRACT III

SMART CARDS: AN ENABLER FOR ARMY PERSONNEL TRANSFORMATION 1

PERSONNEL REDESIGN 2

PERSONNEL REDESIGN IN THE CONTEXT OF THE JOINT ENVIRONMENT 2

DEFENSE INTEGRATED MILITARY HUMAN RESOURCES SYSTEM (DIMHRS) 4

ACCESSING THE NEW PERSONNEL SYSTEM 6

THE COMMON ACCESS CARD 6

THE EVOLUTION OF COMMERCIAL SMART CARDS 7

PRIVATE SECTOR SMART CARDS 7

WHAT DOD SMART CARDS CAN DO 8

INFORMATION SECURITY 10

CONCLUSION 11

ENDNOTES 13

BIBLIOGRAPHY 15

SMART CARDS: AN ENABLER FOR ARMY PERSONNEL TRANSFORMATION

> The magnificence of our moments as an Army will continue to be delivered by our people. They are the engine behind our capabilities and the soldier remains the centerpiece of our formations.
>
> — General Eric Shinseki

A critical element affecting Army readiness is personnel support. Personnel information on the battlefield and across all levels of the Army is necessary to support the force and to enable senior leaders to make wise decisions regarding the force. It gives information to commanders about their soldiers so they can take care of their soldiers while executing operational missions. Personnel support is not exclusively about supporting commanders. It involves the complex processes of recruiting, selecting, processing, classifying, training and sustaining new soldiers, among many others. Personnel support involves accounting for people assigned to the Army, managing their careers, and providing services and supporting well-being for families, retirees and veterans.

Since the beginning of the computer age, the Army has developed many personnel information systems to collect multitudes of data so military personnel managers can provide support to their commanders. But there is no one interoperable system that can meet all personnel needs at all levels of the Army. There is also no one system that can fully support the critical needs of the unified commanders as they execute their responsibilities in the joint nature of warfare today.

The current Army Deputy Chief of Staff for Personnel (DCSPER), advocates that future personnel information management systems must be developed if the Army is to manage the enormous amounts of information needed to sustain itself on the battlefield and across the full spectrum of operations.

This paper addresses emerging personnel information systems, and the status and potential of one enabler for future systems--"smart cards." We will consider the evolution of smart cards in the private sector, addressing the background of the current technology and applications within civilian industry. The paper will outline potential smart card uses for the military with special focus on the Army and its on-going transformation of personnel processes. It is the

intent of this paper to offer ways for the military to use smart card technology efficiently, cost-effectively, and with the greatest value to the warfighter.

PERSONNEL REDESIGN

A major part of the Army's current transformation to the "Army of the future" involves redesign of personnel systems. This redesign is an initiative of the DCSPER to more fully integrate personnel support and improve processes for simpler, yet better results. It involves moving to an easily accessible and comprehensive system for all components of the Army. Personnel redesign will follow the same strategy used for the total Army transformation, that of having an initial, interim and objective plan.

Consistent and accurate access to information is the minimum expectation of the Army force, and changes in information processes are the key to the personnel redesign effort. Future processes must empower soldiers and commanders, eliminate redundancy, and streamline the way we do business. Proponents responsible for current processes must analyze them in terms of redesign and determine what can change by incorporating three principles that drive the process change: 1) Input and verification of data at the action level; 2) No unnecessary review or handling; and 3) Simple, yet effective service.[1]

PERSONNEL REDESIGN IN THE CONTEXT OF THE JOINT ENVIRONMENT

The Goldwater-Nichols Act (GNA) of 1986 provided for "organizational arrangements that will lead to true unity of effort in DoD and in the warfighting commands in the field."[2] By increasing the authority of the CINCs and improving joint officer management, the act changed the way the Services were to interact. Now, CINCs are faced with new personnel information management requirements with real-time information reporting, reinforcing the need for an operating environment of one, fully integrated system. Working to develop an effective personnel system addressing joint needs, the Office of the Secretary of Defense (OSD) personnel managers are confronting some critical issues. Currently, the Services cannot provide essential personnel information to warfighting CINCs using the Services' personnel information systems. There are problems of timely and accurate data, identifying theater personnel assets, lack of personnel visibility/tracking, personnel/pay management inadequacies, and interface problems with separate/different systems for active and reserves. Stovepipe Service-based systems still plague DoD because they cannot interface with other Services.

OSD has been studying the problem of interoperability for more than a decade. The problems with interoperability of Service personnel systems began to emerge as early as 1989 with the initiation of the Defense Information Management Program.[3] The Services began the arduous process of attempting to resolve the problems. However, the task force formed to study the functional and technical inadequacies of DoD's personnel information management systems failed to obtain a clear picture of the scope of the problems. What became clear was that many military personnel systems did not meet the operational requirements of the CINCs and did not eliminate or reduce redundant data collection nor conserve resources, all of which are needed to enhance readiness.[4] Deficiencies during Desert Storm/Desert Shield cited several military personnel management and pay systems and indicated that the Military Personnel Information Management Program (MPIMP) goals were not met.[5] In a report to the Undersecretary of Defense (Personnel and Readiness), proponents characterized these systems as "Service and component personnel systems that support component-specific policies and business practices and use component-specific data elements." [6] The report thus noted that there are different sets of standards and the lack of core standard data elements made it difficult for OSD managers and CINCs to properly integrate information from the Services.[7] Services alone could not resolve personnel systemic problems. The most important reasons were the incompatibility of hardware and software between Services and the reluctance of these personnel communities to fix the problems. For example, the Army core data elements in its legacy personnel systems would not interface with Navy, Air Force, or other DoD databases, and likewise, neither did the others. Interfaced automated personnel information systems were very few, if any. In addition, Congress had mandated certain components, like the Army Reserve, to use a particular personnel information management system.

Then In 1996, DoD developed a strategic vision and issued a directive to the Services mandating migration to information systems that are interoperable with those of other Services.[8] A two-year functional and technical analysis of existing Service personnel information management systems was conducted to determine if any of these systems qualified as the migration system for core military personnel functions. The study revealed major differences in each component that are not interoperable with other component-specific systems and business practices. Because these systems were Service-specific, it would degrade the interface ability of the Services, and prevent integration of each Services policies and objectives into one system.[9] The result was that none of the existing systems could meet the complex data and interface requirements of the other Services or support the current personnel practices of the

other Services. Consequently, DOD's challenge became how to develop a personnel information management system with the desired capability.

OSD personnel managers determined what was needed in a joint personnel information system. First, it should be a system able to pass information back and forth between Service components efficiently. Second, CINCs needed a system that would track soldiers, sailors, marines, and airmen in theater without having tons of duplicative and incorrect data elements. Third, CINCs needed a system that would support their operational requirements.[10] Accordingly, OSD, with Defense Science Board validation, launched the development of the Defense Integrated Military Human Resources System (DIMHRS).[11]

DEFENSE INTEGRATED MILITARY HUMAN RESOURCES SYSTEM (DIMHRS)

DoD's new personnel information management system is DIMHRS.[12] When fully implemented, DIMHRS will provide a single, fully integrated personnel and pay system with standardized data elements that can be used across the spectrum of operations by the Services and CINCs. DIMHRS can generate Service specific modules where needed. It will use Commercial Off the Shelf (COTS) and Government Off the Shelf (GOTS) Software to provide relevant personnel information to the warfighter, while supporting business processes across DoD. All Services have been directed to adopt this single, all component, fully integrated personnel and pay system to resolve past problems. A Military Personnel Joint Requirements Study reinforced OSD's conclusion that the Services could develop common functional requirements to support a DIMHRS prototype system. Standardization and interoperability will be the bottom line objective for DIMHRS.

Implementation of DIMHRS should greatly expand the visibility of soldiers on the battlefield, no matter the component, and should repair the gap between information collection and access deficiencies noted earlier with legacy systems. Additionally, DIMHRS will give military personnel managers the ability to track personnel in and around the Area of Operations (AOR) and will facilitate determination of requirements for replacements and facilitate casualty information. For example, if a soldier is medically evacuated, all of the pertinent information will automatically be transmitted from the medical personnel information system to DIMHRS and then shared with the appropriate action personnel throughout the system.

DIMHRS will be a centralized computer database with front-end application capability using web-based applications. DIMHRS will provide the Service capability to effectively manage service members during peacetime, war, mobilization, and demobilization. Additionally, it will capture relevant and accurate information throughout the system.

When DIMHRS is actually in place, it will replace or subsume the functionality of numerous Service-specific programs like SIDPERS3, the Installation Service Modules (ISM) Suite, and the Army Casualty Information Program (ACIP and ACIP Light).[13] Many other systems and processes will eventually feel the impact of DIMHRS as it matures and assumes more functionality.

There is one significant problem that still must be resolved in DIMHRS: the integration of the Service-specific regulations, policies, doctrines, and terminology into the system, causing the system to be truly "joint." This has been very difficult especially in the area of collecting and transmitting standardized data elements. All Services must work together under the same information technology rules if DIMHRS is to be effective and be the bridge that brings together the Services' disparities.

By taking a long-term approach, the DoD and military Services will be able to build on the DIMHRS personnel information management system by making and updating access easier for the user.

All Services have taken initiatives to improve their personnel information management systems that will complement DIMHRS, making great progress. For the Army, the development and implementation of the Integrated Total Army Personnel Database (ITAPDB) will complement DIMHRS.[14] ITAPDB is a web-based, user-friendly database expected to be fielded in August 2001. ITAPDB will integrate active, reserve and civilian components, provide commanders and military personnel managers the visibility and accountability of service members from each component during mobilization and deployment, and should resolve the automated interface problems that prevent an orderly flow of soldier data across component and field systems boundaries.

ITAPDB will provide the Army a single source for personnel data and should resolve interface problems that have previously interfered with the projection of data across web-based, DoD system boundaries. The good news for military personnel managers is having one corporate database that provides a single view of personnel information in the Army. This one databse, not several, will eventually interface with all Service systems in DoD. Because ITAPDB will be web-based, this will open the system accessibility never known in earlier legacy systems. Accessibility issues and information assurance issues are still being worked but there is attention being given to protecting information from future domestic and foreign enemies.

ACCESSING THE NEW PERSONNEL SYSTEM

How will access to information and applications in DIMHRS and ITAPDB become available to those who need it and are authorized it? Recently, the Deputy Secretary of Defense signed a memorandum directing that DoD adopt the Common Access Card (CAC) or *smart card*, technology.[15] In directing the implementation of the CAC, the Deputy Secretary of Defense developed a strategic plan that contained two goals.[16] First, the DoD wants to achieve global flexibility, increase productivity, and create a dynamic working environment through Electronic Business/Electronic Commerce. Second, DoD desires to achieve efficient and effective responses by rapid introduction of business process improvements and new technologies.[17] Now the use of the smart card is a priority within DoD.[18]

THE COMMON ACCESS CARD

The DoD Human Resource Activity Manpower Data Center issued a preliminary notice of upgrade of the Real Time Automated Personnel Identification System (RAPIDS) and the Defense Enrollment Eligibility Reporting System (DEERS) to incorporate the Common Access Card.[19] Some of the applications included in RAPIDS are capabilities for electronic signature, email, and authentication infrastructure components like firewalls and web servers. The smart card will greatly facilitate interoperability. Using such devices, all Services will continue to develop a comprehensive transition strategy to the transformation vision. After moving to the new system in the transformation, soldiers, sailors, marines and airmen will enjoy quick, on-line access to military personnel applications by using the smart card.

The definition of a smart card as described in the Defense Authorization Act, Section 373(g)(1) is "a credit card-sized device, normally for carrying and use by personnel, that contains one or more integrated circuits and may also employ one or more of the following technologies: (a) magnetic stripe; (b) barcodes (linear or two dimensional); (c) noncontact and radio frequency transmitters; (d) biometric information; (e) encryption and authentication; or (f) photo identification.[20] Both its level of integration and type of interface can expand the use of smart card technology. The level of integration is the programmed amount of integrated functions (as many as DoD wants) contained within the card and the type of interface is how the card communicates externally. Examples of different integration level cards are memory cards, protected memory cards and processor cards. The types of card interfaces are contact, contactless, combination and hybrid.[21]

The primary purposes of the smart card are to serve as the new military identification card and to provide access to DOD facilities and computer systems. The smart card will be the standard identification card for all active duty personnel, Selected Reserve, DoD Civilian employees, and contractors. The card will carry some data directly on the chip and will contain the necessary authentication Certificates that will allow access to web-based systems. The smart card will incorporate the integrated circuit chip and would contain other relevant media as magnetic strip and bar codes.

THE EVOLUTION OF COMMERCIAL SMART CARDS

In 1950, Diners Club and American Express launched their charge cards in the United States, the first "plastic money."[22] However, it was not until the development of the magnetic strip in 1970 that the credit card became part of the information age.[23] In 1974, Roland Moreno of France patented the idea of putting a chip inside a conventional plastic card.[24] Then in 1975, the first memory chip card appeared.[25] This same year, significant applications of smart card technology occurred. Political and economic circumstances were the principal drivers of smart card growth in France because France did not have a viable telecommunications network infrastructure. Consequently, costs of conducting on-line financial transactions were high within France. For those who traveled throughout Europe, the cost of financial transactions was astronomical. Only the very rich could afford to engage in financial transactions outside of European borders. Merchants and bankers were conducting business without access to an on-line authorization that resulted in very high incidents of fraud. The smart card met France's need for on-line access transaction authorization capability and virtually eliminated problems of fraud.[26] Today, smart cards have taken Europe by storm. There is a huge demand for this technology and the conventional computer system is just the springboard to futuristic applications.

PRIVATE SECTOR SMART CARD

The current smart card market can be characterized by applications developed within individual industries. Industries are taking advantage of the smart card technology for information storage, management, transmission, and access in some examples discussed below. Customers have access to these features by using a smart card and a decoder whether they are at home or at the office.

In the banking industry, the uses are virtually endless. Financial institutions issue smart cards that have a stored value/electronic purse, physical and logical access, identification for corporate services applications, and for account holders to access their accounts and perform certain on-line transactions from their home or office. By 2010, bank cards may contain pay records, state and federal income tax information, savings accounts, e-checking accounts, pension records, and social security information.

Smart cards are being used in the medical field to allow patients to pay health insurance premiums, medical and dental bills, and file for claims with private insurance companies. In some cases, the medical officer may have instant access to the patient's medical and dental records.

In the telecommunications field, smart cards are being used for no-cash telephones, Internet, and other computer systems access. For television and cable service, a smart card is being used to allow the consumer the ability to enable or disable the scrambler box attached to the television.

Smart cards are being used in the travel/entertainment area. Airlines are using smart cards for ticketless travel, boarding passes, and access to bonus programs. Hotels are using smart cards to identify special customers and for paperless check-ins/outs.

Colleges and universities are allowing students to pay for college tuition, books, room and board, and meals during the semester. The administrative offices are using the smart cards as a method of identification of students and to record financial transactions and transcripts.

Some State driver's license bureaus are issuing automated drivers licenses that may be programmed to pay for tolls, and may eventually contain an individual's driving record that can interface with any law enforcement agency in the United States.

In the retail industry, merchants are able to track their best (and worst) customers and the ones who are loyal to a particular store or brand of merchandise.

The Internet is the most recent industry that is taking advantage of smart card technology. With a smart card, the user is provided secure access to the Internet for purchasing goods by using the integrated microchip and home-scanning device.

WHAT DOD SMART CARDS CAN DO

Military Services will initially focus smart card use on identification purposes. Basically, this card will be used to prove that you are the person you say you are.[27] This will be especially helpful when entering into certain security conscious computer programs like email, the Internet, pay, and health records. The chip on the card can be programmed to allow the card holder

access to other computer systems, facilities, privileges like Morale, Welfare and Recreation (MWR) facilities, telephone access, etc. It can also be programmed to disallow entry into certain facilities, buildings, and computer-accessed programs. For example, the Post Exchange has a severe problem of people issuing checks for insufficient funds. If a patron has had privileges withdrawn due to repeated returned checks for insufficient funds, the card can be updated by the RAPIDS system or a scanner at the Post Exchange disallowing any further purchases for a predetermined amount of time. Another example of the information that can be written on the card can be used by the Military Police. When making a stop for a possible moving violation, the Military Police will be able to scan the person's card with a portable scanner to retrieve vital information concerning the person and the vehicle from a centralized database. The card can retrieve the violator's personal information as well as vehicle registration information, a record of past moving violations and any other law enforcement information they may need.

Currently, the smart card will be used for access to futuristic systems in the "Army of the future." Futuristic applications are already being examined by the Services [28] and specifically, the Army has potential uses of the CAC in several areas. Some of those areas are an Automated Battle Book System, Weapons Issuance System, Automated Arms Rooms System, Legal Assistant Client Services System, and many others. No one system has been selected because all are in the testing and evaluation stage today. In the personnel arena, the CAC is being considered for access to Soldier Applications Systems that will be web-based, enabling the soldier access to certain military personnel processes. For example, the Army is currently testing the DD Form 93 (Record of Emergency Data) in this system to allow a soldier to update his DD Form 93 at home or any other location. Additionally, it can allow access to routine military personnel actions with electronic signature capabilities. A good example of this is requesting a personnel action like assignment to overseas, applying to be considered under the Married Army Couples Program or attendance at Officer Candidate School. If this system is enabled with electronic signature capability, this request can progress from the soldier, through his chain of command, without anyone actually signing or touching the document. One of the greatest benefits of this process is making the current system totally paperless. Another example for potential use of the card is tracking personnel tempo (PERSTEMPO) of soldiers.

Future military personnel S-1 sections could use the smart card in many ways. For example, if a soldier goes to the clinic and is placed on quarters, the old system required a hand-written sick call slip to the First Sergeant and/or S1. By using the CAC, the S-1 would generate an action that would be transmitted to the medical facility. If the clinic places the soldier on

quarters, the clinic simply enters the information into their computer system that would automatically update the soldier's smart card and transmit the information back to the S1. This would automatically generate a "duty status change" in the system without any paper or manual signature.

Across the Services, the Air Force and Navy have predicted some future applications for the smart card. The Navy is testing the smart card's ability to help track ordnance it issues to ships and aircraft and keep headcount in food service facilities for resupplying food based upon the number of personnel that used the dining facility. The Air Force potentially will use the smart card to track pilots, flight hours, physicals, and reassignments of aviators. They are also looking at possible uses in their logistics functions and military personnel applications function. Additionally, DoD is studying the smart card with an open architecture that will enable all agencies in government the ability to use the smart card for a myriad of uses.

By 2010, the smart card should be integral for all Services. This technology will not only include all military Services but the retired population as well. According to Bernard Rotsker, the Under Secretary for Defense for Personnel and Readiness, the CAC will put DOD on the forefront of e-commerce and security.[29]

Smart cards will provide the Army with a way to "bridge" one system to the other Services. The smart card must be able to "talk" to other networked systems. Smart cards can provide information security and confidentiality of personal information. Previously, there had not been a viable system in place that would offer a high level of protection.

INFORMATION SECURITY

The General Accounting Office (GAO) released a report in August 1999 stating, "serious weaknesses in DOD information security continue to provide both hackers and hundreds of thousands of unauthorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive DoD data."[30] If DoD does not resolve this problem, serious repercussions could result that could impair DoD's ability to support the CINCs.

According to the report, control was the most significant weakness in DOD. Access controls are to be managed on a "need-to-know" basis. Further, password management was still weak and users were not required to change their passwords often enough and in some cases were never required to change them at all. User accountability was weakened by the use of generic (group) user accounts instead of single accounts by one user. Military personnel managers using the smart card must take serious security precautions, in light of this report. If confidentiality of personal information has always been a concern in DoD, it has not necessarily

been properly protected in view of the above GAO report. Up to now, DoD has not had a reliable system in place that would offer a high level of protection for the user or the system. The smart card can help solve this information assurance problem with necessary emphasis.

Each CAC user will have an access code and password that will offer a great degree of security. Smart cards can be further used to add biometric capability like fingerprint or retina scanning, as identification means.

One effort to protect information on the CAC has already been completed. The CAC is programmable to void all information on the chip when entering the wrong access code or password. Another important aspect of information security involves making changes to and transmission of data through the users RAPIDS/DEERS account. The information will be protected by a firewall and auto-encrypted when sent through the server to the mainframe.[31]

CONCLUSION

Emerging 21st Century technologies are aiding the Army's transformation to the objective force. Technological advancements such as the smart card will significantly enhance the Army's ability to provide a more lethal, survivable, sustainable, deployable, and mobile force. Advanced technologies will provide our leaders the ability to "see deep" and to achieve "superior situational dominance" with personnel and other information. Employing smart card technology is one aspect of keeping pace with the demand for accurate and timely military personnel information on the battlefield.

The Army is taking great strides toward reducing the demands against resources by developing applications for smart cards. From these efforts, a great deal of success has been achieved. The potential for smart cards is phenomenal. They will allow reduced paperwork and increased unit readiness by eliminating processes that are no longer required as they were in the "stubby pencil" era. Commanders on the battlefield will see timely and accurate information flow and OSD and Army personnel managers will discover greater storage of information and effective uses of the CAC in all environments.

Smart cards, while relatively inexpensive, can pose significant costs in development and maintenance if not resourced wisely. It is very important that the Army develop repeatable processes and policies that can be used and refined in the CAC. Leveraging multiple applications on the same card can provide savings versus issuing a card for every application. Also, the Army must be careful in its approach to alleviate any lack of consistency in DoD smart cards and must move away from developing too many custom smart cards with different levels of interoperability.

Based on recent DoD guidance, it is imperative that the Army work quickly and effectively to develop and implement its CAC strategy. It must also, though, implement its strategy in a focused and thoughtful manner taking into account the unique needs, policies and requirements of the Service and the unified commander. By leveraging the uses of the smart card from civilian industry, the Army can develop its strategy in an efficient, cost-effective way that will provide the best technology and services to the warfighter and consequently, support Army Transformation in a dramatic way.

WORD COUNT=4508

ENDNOTES

[1] "Personnel Redesign", briefing slides with scripted note pages, PERSCOM, US Army Total Army Personnel Command, Alexandria, VA, 2 February 2001.

[2] James R. Locher III, "Building On the Goldwater-Nichols Act", (Washington: National Defense University, 1996), 1.

[3] Office of the Undersecretary of Defense (Personnel and Readiness) Information Management Office. Military Personnel and Readiniess Information Management Program Business Process Reengineering Strategic Plan. Washington: Office of the Undersecretary of Defense (Personnel and Readiness) Information Management Office, 1996.

[4] Ibid., 3.

[5] Ibid., 3.

[6] Ibid., 2.

[7] Ibid., 4.

[8] Office of the Under Secretary of Defense (Personnel and Readiness) Information Management Office, Business Process Reengineering Strategic Plan, (Washington: Office of the Under Secretary of Defense (Personnel and Readiness) Information Management Office, 1996), 2.

[9] Ibid, 1.

[10] "Office of the Under Secretary of Defense (Personnel and Readiness) Joint Requirements and Integration Office," 18 December 2000; available from http://www.mpm.osd.mil. Internet. Accessed 21 January 2001.

[11] "Defense Integrated Military Human Resources System (DIMHRS) Project Overview," 18 December 2000; available from http://www.mpm.osd.army.mil/dimhrs.htm. Internet. Accessed 27 January 2001.

[12] Ibid., 3.

[13] Ibid., 5.

[14] Total Army Personnel Command, "ITAPDB Vision," 9 December 2000; available from http://www,perscom.army.mil/tagd/transition/itapdb.htm. Internet. Accessed 21 January 2001.

[15] Under Secretary of Defense John J. Hamre, "Smart Card Adoption and Implementation," memorandum for Secretaries of the Military Departments, Washington, D.C., 10 November 1999.

[16] Linda Hardin hardinl@monroe.army.mil. "Army Begins Testing Computerized ID Card," electronic mail message to James L. Call, Jr. James.Call@Carlisle.army.mil. 11 October 2000.

[17] Under Secretary of Defense John J. Hamre, "Smart Card Adoption and Implementation," memorandum for Secretaries of the Military Departments, Washington, D.C., 10 November 1999.

[18] Ibid., 2.

[19] Office of the Secretary of Defense, Human Resource Activity Center, Defense Manpower Data Center, Department of Defense (DOD) Real-Time Automated Personnel Identification System (RAPIDS) LRA Certification Practice Statement (CPS) (Washington: Office of the Secretary of Defense, 2000), 1.

[20] Office of the Deputy Secretary of Defense, "Smart Card Environment Paper," draft memorandum, Washington, D.C., 20 February 2001.

[21] Ibid., 3.

[22] "History of Credit Cards," 1 November 2000; available from http://www.didyouknow.com/creditcards.htm; Internet. Accessed 21 January 2001.

[23] Ibid.

[24] Ibid.

[25] Ibid.

[26] Ella Nichols nicholse@Carlisle.army.mil, "Smart Card Environment Paper," electronic message to James L. Call, Jr. James.Call@Carlisle.army.mil, 25 January 2001.

[27] Linda D. Kozaryn, "Common Access Cards Will Save Time," The Carlisle Barracks Banner, (October 2000) 10.

[28] Ibid.

[29] Ibid.

[30] General Accounting Office, Department of Defense (DOD) Information Security-Serious Weaknesses continue to Place Defense Operations At Risk (Washington, D.C. U.S. General Accounting Office, September 1999), 25-37.

[31] Ibid., 25-39.

BIBLIOGRAPHY

"Personnel Redesign", briefing slides with scripted note pages, PERSCOM, US Army Total Army Personnel Command, Alexandria, VA, 2 February 2001.

Locher, James R. III, "Building On the Goldwater-Nichols Act," (Washington: National Defense University, 1996), 1.

U.S. Office of the Undersecretary of Defense (Personnel and Readiness) Information Management Office. Military Personnel and Readiniess Information Management Program Business Process Reengineering Strategic Plan. Washington: Office of the Undersecretary of Defense (Personnel and Readiness) Information Management Office, 1996.

U.S. Office of the Under Secretary of Defense (Personnel and Readiness) Information Management Office, Business Process Reengineering Strategic Plan, (Washington: Office of the Under Secretary of Defense (Personnel and Readiness) Information Management Office, 1996), 2.

U.S.Office of the Under Secretary of Defense (Personnel and Readiness) Joint Requirements and Integration Office," 18 December 2000; available from http://www.mpm.osd.mil. Internet. Accessed 21 January 2001.

"Defense Integrated Military Human Resources System (DIMHRS) Project Overview," 18 December 2000; available from http://www.mpm.osd.army.mil/dimhrs.htm. Internet. Accessed 27 January 2000.

U.S. Total Army Personnel Command, "ITAPDB Vision," 9 December 2000; available from http://www,perscom.army.mil/tagd/transition/itapdb.htm. Internet. Accessed 21 January 2001.

U.S. Under Secretary of Defense John J. Hamre, "Smart Card Adoption and Implementation," memorandum for Secretaries of the Military Departments, Washington, D.C., 10 November 1999, 1.

Hardin, Linda, hardinl@monroe.army.mil. "Army Begins Testing Computerized ID Card," electronic mail message to James L. Call, Jr. James.Call@Carlisle.army.mil. 11 October 2000.

U.S. Under Secretary of Defense John J. Hamre, "Smart Card Adoption and Implementation," memorandum for Secretaries of the Military Departments, Washington, D.C., 10 November 1999, 4.

U.S. Office of the Secretary of Defense, Human Resource Activity Center, Defense Manpower Data Center, Department of Defense (DOD) Real-Time Automated Personnel Identification System (RAPIDS) LRA Certification Practice Statement (CPS) (Washington: Office of the Secretary of Defense, 2000), 1.

U.S. Office of the Deputy Secretary of Defense, "Smart Card Environment Paper", draft

memorandum, Washington, D.C., 20 February 2001.

"History of Credit Cards," 1 November 2000; available from http://www.didyouknow.com/creditcards.htm; Internet. Accessed 21 January 2001.

Nichols, Ella J., nicholse@Carlisle.army.mil, "Smart Card Environment Paper," electronic message to James L. Call, Jr. James.Call@Carlisle.army.mil, 25 January 2001.

Kozaryn, Linda D., Common Access Cards Will Save Time, The Carlisle Barracks Banner, (October 2000) 10.

U.S. General Accounting Office, Department of Defense (DOD) Information Security-Serious Weaknesses continue to Place Defense Operations At Risk (Washington, D.C. U.S. General Accounting Office, September 1999), 25-37.